United States
Department of
Agriculture

Operations
and Finance

Regulations for Classification, Declassification, and Safeguarding Classified Information

Form AD–796 (6/81)

TABLE OF CONTENTS

CHAPTER 1

General Provisions

CHAPTER 2

Responsibility for Safeguarding Classified Information

CHAPTER 3

Classification of National Security Information

CHAPTER 4

Declassification and Downgrading

CHAPTER 5

Access, Dissemination, and Accountability of Classified Material

CHAPTER 6

Storage of Classified Material

CHAPTER 7

Protection of Security Storage Equipment and Controlled Area

CHAPTER 8

Reproduction of Classified Material

CHAPTER 9

Transmission of Classified Information and Material

CHAPTER 10

Disposition or Destruction of Classified Information

CHAPTER 11

Security Violations and Compromise of Classified Material and Information

CHAPTER 12

Security Education Program

CHAPTER 13

Program Management

Chapter 1

General Provisions

101 FOREWORD

The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizency is reflected in the Freedom of Information Act, the Privacy Act, and in the current public information policies of the executive branch as prescribed in Executive Order 12065.

Within the Federal Government, however, there is some classified material and information which, because it bears directly on the effectiveness of our national security and the conduct of our foreign relations, must be safeguarded for the security of the United States and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is our duty, both as USDA employees and as citizens, that such classified material and information be given only limited dissemination. Such classified material and information is expressly exempted from mandatory public disclosure by Section 552(b) (1) of Title 5, United States Code.

To insure that such classified material and information is safeguarded, but only to the extent and for such period as is necessary, this Handbook identifies the material to be safeguarded, prescribes classification, downgrading, declassification, and safeguarding procedures to be followed, and establishes a monitoring system to insure its effectiveness.

The regulations set forth in this Handbook are intended to achieve a coordinated and uniform policy throughout USDA in the classification, declassification, and safeguarding of classified material. The regulations apply to all classified material in the custody of USDA regardless of whether the material was originated within USDA or released to it. This Handbook supersedes the "Regulations for Classification, Declassification, and Safeguarding Classified Information" issued in 1974.

102 SCOPE

All employees of USDA, including individuals serving in an advisory or consultative capacity, are subject to the regulations and procedures set forth herein. Failure on the part of the employees of USDA to observe these regulations constitutes grounds for disciplinary action, including dismissal. USDA personnel entrusted with classified material and information

furnished by a foreign government or by international organizations of Governments are cautioned to contact the Department Security Officer for details concerning specialized security requirements.

103 DEFINITIONS

For the purposes of this Handbook, the following definitions of terms shall apply. (In addition to the terms explained below, other terms commonly used in the Department of Defense Industrial Security Program are explained in the Industrial Security Manual for Safeguarding Classified Information DOD 5220.22M)

Access means the ability and opportunity to obtain knowledge or possession of classified information. An individual does not have access to classified information merely by being in a place where information is kept. Access is restricted by a determination of a need-to-know and a determination of trustworthiness.

USDA Agency - means a major line or program unit of the Department headed by an Administrator or equivalent who reports to the Secretary, Deputy Secretary, Under Secretary, Assistant Secretary, or Group Director.

Agency includes any executive department, military department, intelligence agency, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

USDA Agency Head means the Administrator or the Chief Executive Officer of a USDA agency in the Department.

Agency Classified Material Control Officer is the Security Officer of an Agency in the National Headquarters.

Authorized Individuals are those persons who have a need-to-know for the classified information involved, and who have been determined to be trustworthy by the Department Security Officer based on the results of an appropriate investigation.

Classification (Original) means the initial determination that information requires protection against unauthorized disclosure in the interest of national security and a designation of the level of classification.

Classification Guides are documents issued in an exercise of authority for original classification that include determinations with respect to the proper level and duration of classification of categories of classified information.

Classifier means for USDA an individual who makes a derivative classification determination and applies a security classification to official information. A USDA classifier may assign a derivative security classification based either on a properly classified source or a classification guide received from the Department which originally classified the information.

Clearance means an administrative determination under the provisions of DPM 732 by competent authority that an individual has been adjudged eligible for access to classified information of a specified category.

Compromise means a breach of security which results from an unauthorized person obtaining knowledge of classified information. Affected material is not automatically declassified.

COSMIC is a special marking which indicates that the information is the property of NATO and subject to special security controls.

Custodian is an individual who has possession or is otherwise charged with the responsibility for safeguarding and accounting for classified material.

Declassification means a determination that classified information no longer requires, in the interest of national security, a degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

Derivative classification means that information used in a new document is in substance the same information currently classified in a source document or classification guide. The extracted information used in the new document must be classified at the same level as in the source document.

Disclosure means an officially authorized release or dissemination by competent authority whereby the information is furnished to a specific individual, group, or activity.

Disseminate means to furnish classified material under continued control of the U.S. Government to persons having a proper clearance and a "need-to-know" e.g. to another U.S. Government agency or Department or to a contractor.

Document means any recorded information regardless of its physical form or characteristics including, but not limited to, the following: All written material, whether handwritten, printed, or typed; and painted, drawn, or engraved material; all sound or voice recordings; all printed photographs and exposed or printed film, still or motion pictures; and all reproduction of the foregoing, by whatever process reproduced.

Downgrade means to determine that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

Foreign Government Information is (a) information provided to the United States by a foreign government or international organization of governments in the expectation, expressed or implied, that the information is to be kept in confidence; or (b) information produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement, or both, be kept in confidence.

Formerly Restricted Data is information removed from the Restricted Data category upon determination jointly by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. Such information is treated the same as Restricted Data for purposes of foreign dessemination.

For Official Use Only (FOUO) is an administrative marking applied to official information which requires protection in accordance with statutory requirements or in the public interest, but which is not within the purview of the rules for safeguarding information in the interest of national security. Such information is not within the purview of this Handbook.

Industrial Security means that portion of the industrial security program which is concerned with the protection of classified information in the possession of U.S. industry.

Information Security means safeguarding information against unauthorized disclosure, or, the result of any system of administrative policies and procedures for identifying, controlling, and protecting such information from unauthorized disclosure, the protection of which is authorized by Executive Order or statute.

Intelligence means the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of foreign operations, and which is immediately or potentially significant to military planning and operations.

Inventory is a procedure employed to verify accountability of classified material by comparing entries on a register against the document of entry on the record of destruction or a signed receipt.

Material means any document, product, or substance on or in which information may be recorded or embodied.

National Security is the national defense and foreign relations of the United States.

NATO Classified Information is the term applied to all classified information circulated within and by NATO whether such information originates in the organization itself or is received from member nations or from their international organizations.

Need-to-know is a term given to the requirement that the dissemination of classified information be limited strictly to those persons whose official or other governmental duties require knowledge or possession thereof. No person is entitled to knowledge or possession of classified information solely by virtue of his/her grade, office, or security clearance. Responsibility for determining whether a person's duties require that he/she is authorized to receive it rests upon each individual who has possession, knowledge, or control of the information involved and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency, or a foreign government.

Official Information is information which is owned by, produced by, or is subject to the control of the United States Government.

Restricted Data is that data which is defined in Section 11(y) of the Atomic Energy Act of 1954, as amended as "all data concerning: (1) Design, manufacture or utilization of atomic weapons, (2) the production of special nuclear material, or (3) the use of special nuclear material in the production of energy, but to include data declassified or removal from RESTRICTED DATA Category pursuant to Section 142."

Short Title is a designation applied to a classified document, project, material, or device for purposes of security and brevity. It consists of figures, letters, words, or combination, thereof, without giving any information relative to classification or content of the document, material, project, or device. It may include, for example, the first letter of each word of the subject of the document.

Unauthorized Person is any person not authorized access to specific classified information, irrespective of that person's eligibility for such access (e.g. possession of an appropriate clearance).

Unbound Documents means material such as letters, memoranda, reports, telegrams, and similar documents, the pages of which are not permanently and securely fastened together.

Upgrade means to determine that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher degree.

Chapter 2

Responsibility for Safeguarding Classified Information

201 DEPARTMENT RESPONSIBILITY

The Department Security Officer is responsible for planning and directing a Department-wide administrative program for the classification, declassification and safeguarding of classified material in the possession of USDA, including the development and publication of minimum standards, procedures, specification, and guidelines in connection herewith. He/she will assure that active training and orientation programs are maintained for employees concerned with classified material. The Department Security Officer shall insure effective compliance with the implementation of the Executive Order and shall chair the Department Review Committee which shall have authority to act on all suggestions and complaints with respect to the Department's administration of the Order.

202 AGENCY RESPONSIBILITY

1. Agency Head - Each agency head is directly responsible for safeguarding all classified material within his/her jurisdiction and control. He/she must initiate and supervise measures or instruction necessary to insure effective control at all times in line with Department policy and regulations. He/she must also insure that any employee who must have access to such classified material in pursuit of his/her position is appropriately cleared prior to assignment to the position. An agency head may delegate authority to perform security control functions charged to him/her, but he/she may not delegate his/her assigned responsiblity. Security is a responsibility of leadership.

2. Agency Classified Material Control Officer

(a) The head of each agency shall designate a responsible employee of the agency to serve as the Agency Classified Material Control Officer. He/she will be responsible to the agency head for maintaining adequate facilities, procedures, and controls for safeguarding classified material coming within the custody of the agency. He/she is also responsible for maintaining an active program of orientation and training to keep employees informed concerning these regulations, and to impress upon them their individual responsiblity for exercising vigilance and care in safeguarding classified material.

(b) Each Classified Material Control Officer shall maintain a current record of all employees in his/her agency who have been cleared and authorized to have access to classified material. This Officer shall promptly advise the Department Security Officer when one of these employees leaves the service of his/her agency.

(c) The loss or compromise of classified material or information shall be promptly reported to the Department Security Officer

(d) Neither the Classified Material Control Officer nor any other employee, regardless of grade or position, shall advise other agencies or establishments outside the Department concerning the level of security clearance of an employee. Such information will be furnished by the Department Security Officer.

3. USDA Field Offices and Installation - Employees in charge of field offices and installations are responsible for insuring the adequate protection of classified material in the possession of their respective offices and installations, including component activities geographically located apart from the parent office or installation, in accordance with the provisions set forth in this Handbook.

203 EMPLOYEE RESPONSIBILITY

1. Each supervisor of a USDA division, office or other organizational unit to which classified material is entrusted will be responsible for insuring that:

(a) All such material is provided adequate safeguarding at all times and under all circumstances.

(b) Each USDA employee under his/her supervisor and/or each non-USDA employee present is adequately instructed in and fully complies with all of the pertinent provisions of this Handbook and such other requirements as may be established by the Classified Material Control Officer.

2. Each USDA Employee Who has Reasons to Believe That:

(a) A practice of condition exists which fails to provide for adequate safeguarding of any classified material will report the circumstances promptly to his/her immediate supervisor.

(b) The loss of compromise of classified material or information will be promptly reported to the Agency Classified Material Control Officer.

3. Each USDA employee to whom classified material has been entrusted will:

(a) Follow each procedure established by his/her Agency Classified Material Control Officer for the purpose of preventing unauthorized access to classified material.

(b) Be responsible for insuring that the material in his/her possession or custody is kept in approved security storage equipment.

(c) Prior to giving a prospective recipient access to classified material or information, insure that he/she has both:

(1) a security clearance to at least the same category of classification as the material or information involved; and

(2) a valid need-to-know in connection with his/her official duties.

(d) Be responsible to challenge through mandatory review and other appropriate procedures, those classification decisions believed to be improper.

(e) Prior to termination of employment or contemplated temporary separation for a sixty-day period or more, or reassignment to a non sensitive position within the Department, an employee shall be briefed concerning his/her obligations with regard to maintaining security of classified national security information obtained during his/her service in the Department, and to bring to his/her attention the applicable statutory requirements in this connection. He/she shall be required to read and execute form AD-491 "Security Debriefing Secrecy Agreement" in the presence of the Agency Classified Material Control Officer. He/she should be required, at that time, to surrender or account for any classified material in his/her personal possession or custody.

Classification of National Security Information

301 SECURITY CLASSIFICATION CATEGORIES

Official information or material which requires protection against unauthorized disclosure in the interest of the national security or foreign relations of the United States is classified in one of three categories; "Top Secret," "Secret," or "Confidential," depending upon the degree of its significance to the national security. No other categories shall be used to identify official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

1. "Top Secret" refers to that national security information or material which requires the highest degree of protection. The test of assigning "Top Secret" classification shall be whether unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national security plans or complex cryptologic and communications intelligence systems; the revelation of scientific or technological developments vital to national security. The classification shall be used with the utmost restraint.

2. "Secret" refers to that national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.

3. "Confidential" refers to that national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause identifiable damage to the national security.

302 AUTHORITY TO CLASSIFY

1. USDA Officials - USDA officials do not have original classification authority for information or material that is created within the Department.

2. Excepted Case - Should a USDA employee originate information believed to require original classification, the information shall be protected in the manner prescribed by the Executive Order 12065 and appropriate Department directives. The information shall be forwarded promptly to the Department Security Officer who shall transmit the document(s) to the department or agency which has appropriate subject matter interest and original classification authority. The Order provides that the department or agency shall decide within thirty (30) days whether to classify the information. When it is not clear which agency should receive the information, it shall be sent to the Director of the Information Security Oversight Office for a determination.

303 DURATION OF CLASSIFICATION

National security information when originally classified shall have a date or event for automatic declassification no more than six years later. Only officials with Top Secret classification authority may classify information for more than six years from the date of the original classification. In such cases, the identity of the official who authorizes the extension shall be shown on the document.

304 DERIVATIVE CLASSIFICATION

1. Responsibility

(a) Derivative application of classification markings is the responsibility of those USDA employees who incorporate, paraphrase, restate, or generate in new form, information which is already classified or those who apply markings in accordance with a classification guide.

(b) Employees who apply derivative classification markings shall:

(1) Respect original classification decisions;

(2) Verify the information's current level of classification so far as practicable before applying the markings; and

(3) Carry forward to any newly created documents, the assigned dates or events for declassification or review and any additional authorized markings. Where checks with the original classification authority of a source document result in no change in the classification of the source document, the new document shall be marked accordingly.

(c) Employees who have created a document requiring derivative classification should consult with the Department Security Officer for guidance when necessary.

(d) The ACMCO will forward a report two (2) times a year (April 15 and October 15) to the Department Security Officer providing the number of derivatively classified documents created by his/her agency. This reporting procedure is necessary to assist the Department Security Officer in monitoring the application of the provisions of Executive Order 12065 and providing required reports to the Director, Information Security Oversight Office (ISOO).

2. Marking Derivatively Classified Documents (See Example Page 1 and 2

(a) Paper copies of derivatively classified documents shall be marked at the time of preparation as follows:

(1) The classification authority shall be shown on a "classified by" line, e.g. "classified by (insert identity of classification guide)" or "classified by (insert identity of original classification)." If the classification is derived from more than one source, contact the Department Security Officer for guidance.

(2) The date and identity of the Department of the source document shall be shown on the document.

(3) Dates or events for declassification or review shall be carried forward from the source material or classification guide and shown on a "declassify on" or "review for declassification on" line. If the declassification is derived from more than one source, the latest date for declassification or review applicable to the various source materials shall be applied to the new information.

(4) One of the three classification designations (Top Secret, Secret, or Confidential), shall be stamped at both the top and bottom of each page containing classified information.

3. Transmittal Documents

A transmittal document shall indicate on its face the highest classification of information being transmitted and the classification, if any, of the transmittal document. An unclassified transmittal should bear the notation "unclassified upon removal of enclosure."

4. Marking foreign government information

Except in those cases where such markings would reveal intelligence information, foreign government information incorporated in United States documents shall, whenever practical, be identified in such manner as to assure that the foreign government information is not declassified prematurely or made accessible to nationals of a third country without consent of the originator. Documents classified by a foreign government or an international organization of governments will, if the foreign classification is not in English, be marked with the equivalent U.S. classification.

5. Prohibitive Markings

(a) Only the designations "Top Secret," "Secret" or "Confidential" as prescribed by the Order may be used to identify classified information. Markings such as "For Official Use Only" and "Limited Official Use" shall not be used for that purpose. Terms such as "Conference" or "Agency" may not be used in conjunction with the derivative classification designations; e.g., "Agency Confidential" or "Conference Confidential."

(b) Classification shall not be used to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization or Agency; or to restrain competition.

(c) Basic scientific research information not clearly related to the national security shall not be classified.

(d) References to classified documents that do not disclose classified information shall not be classified or used as a basis for classification.

(e) Classification shall not be used to limit dissemination of information that is not classifiable under the provisions of Executive Order 12065 or to prevent or delay the public release of such information.

(f) No document originated on or after December 1, 1978, shall be derivatively classified after a USDA Agency has received a request for the document under the Freedom of Information Act or the mandatory review provisions of the Order unless such classification is consistent with the provisions of the Order, and is authorized by both the USDA Agency Head and the Department Security Officer.

(g) Classification shall not be restored to documents already declassified and released to the public under Executive Order 12065 or prior Orders.

6. New Materials.

(a) New material that derives it classification from information classified on or after December 1, 1978, shall be marked with declassification date or event, or the date for review, assigned to the source information.

(b) New material that derives its classification from information classified prior to December 1, 1978, shall be treated as follows:

(1) If the source material bears a declassification date or event twenty years or less from the date of origin, that date shall be carried forward on the new material.

(2) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification beyond thirty years, the new material shall be marked for review for declassification at thirty years from the date of original classification of the source material.

Chapter 4

Declassification and Downgrading

401 DECLASSIFICATION

(1) Declassification of information shall be given emphasis comparable to that accorded classification. Information classified pursuant to the Order and prior Orders shall be declassified as early as national security considerations permit. Decisions concerning declassification shall be based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event which permits declassification. When information is reviewed for declassification pursuant to the mandatory review procedures of the Order or the Freedom of Information Act, it shall be declassified unless the declassification authority established pursuant to Section 4 02 of the Order determines that the information continues to meet the classification requirements prescribed in the Order despite the passage of time.

(2) Should the Director of the Information Security Oversight Office determine that information originally classified in the past by USDA officials is classified in violation of E.O. 12065, the Director may require the agency that classified the information to declassify it. Any such decision may be appealed through the Department Security Officer to the National Security Council.

402 AUTHORITY TO DOWNGRADE AND DECLASSIFY

(1) The authority to downgrade and declassify national security information originally classified within USDA shall be exercised as follows:

(a) By the Secretary of Agriculture; Deputy Secretary; Under Secretary for International Affairs and Commodity Programs; each Assistant Secretary; each Deputy Under Secretary; and Deputy Assistant Secretary within the Office of the Secretary with respect to all information over which their respective offices exercise jurisdiction.

(b) By the USDA official who authorized the original classification if that official is still serving in the same position, by a successor, or by a designated supervisory official of either.

(c) By the Department Security Officer or official at the division chief level as a result of their professional knowledge of the subject matter as it relates to the national security.

403 TRANSFERRED INFORMATION

1. For classified information transferred in conjunction with a transfer of functions - not merely for storage problems - the receiving agency shall be deemed to be the originating agency for all purposes under Executive Order 12065.

2. For classified information not transferred in accordance with Paragraph 403-1, but originated in an agency which has ceased to exist, each agency in possession shall be deemed to be the originating agency for all purposes under the Order. Such information may be declassified or downgraded by the agency in possession after consulting with any other agency having an interest in the subject matter.

3. Classified information transferred to the General Services Administration for accession into the Archives of the United States shall be declassified or downgraded by the Archivist of the United States in accordance with the Order, the directives of the Information Security Oversight Officer, and pertinent regulations of this Department.

404 SYSTEMATIC REVIEW DECLASSIFICATION GUIDELINES

1. Policy

(a) The Department Security Officer shall prepare and keep current such guidelines as are required by the Order for the downgrading and declassification of USDA-originated material that is twenty (20) years old or older.

2. Systematic Review Procedures

(a) Information originally classified by USDA, shall be reviewed for declassification as it becomes twenty (20) years old. Transition to systematic review at twenty (20) years shall be implemented as rapidly as practicable and shall be completed by December 1, 1988.

(b) USDA classified non-permanent records which are scheduled to be retained for more than twenty (20) years need not be systematically reviewed, but shall be reviewed for declassification upon request.

(c) USDA classified information constituting permanently valuable records of the Government as defined by 44 U.S.C. 2103 and information in the possession and control of the Administrator of General Services pursuant to the 44 U.S.C. 2107 and 2107 Note shall be reviewed for declassification as it becomes twenty (20) years old by the Archivist of the United States with the assistance of Department personnel deignated for the purpose. In the case of twenty (20) year old material in the custody of USDA agencies, such review shall be accomplished by each Agency Classified Material Control Officer.

405 MANDATORY REVIEW FOR USDA ORIGINALLY CLASSIFIED DOCUMENTS

1. Information Covered

(a) All information originally classified within USDA under prior Executive Orders, except information described in Section 3-503 of the Order, is subject to mandatory review for declassification upon a request from a member of the public, a Government employee or from agencies to declassify and release such documents under the provisions of the Order. Such request shall be reviewed by the Department Security Officer and the USDA Agency responsible for the original classification in accordance with the procedures of this section.

2. Submission of Requests for Review

(a) Requests for mandatory review of classified information shall be submitted in accordance with the following:

(1) Requests originating within USDA shall in all cases be submitted directly to the Department Security Officer, for review and a declassification determination.

(2) Requests from a member of the public or other agencies may direct requests for mandatory review of classified information under the Order to the Department Security Officer, Office of Personnel, Administration Building, U.S. Department of Agriculture, Washington, D.C. 20250. The Security Officer shall, in turn, refer the request to the appropriate USDA Agency Head for action.

3. Requirements for Processing

(a) Requests for declassification review and release of information shall be processed in accordance with the provisions of this section, subject to the following conditions:

(1) The request is in writing and reasonably describes the information sought.

(2) Whenever a request does not reasonably describe the information sought, the USDA Agency shall notify the requestor that unless additional information is provided or the scope of the request is narrowed, no further action shall be undertaken.

(3) Requests for mandatory review shall be acted upon within sixty (60) days after the request is mailed.

(4) If the request requires the rendering of services for which fees may be charged pursuant to 31 U.S.C. 438a, the requester shall be so notified before the service is rendered.

4. Requests for Information Classified by Another Agency

When a USDA Agency receives a request for declassification of information in a document which is in the custody of the USDA Agency which was classified by another agency, the USDA Agency shall refer the request to the classifying agency together with a copy of the document containing the information requested when practicable, and shall notify the requester of the referral and that a response will be sent to the requester by the agency which was sent the referral. When a USDA Agency receives such a referral, it shall process the request in accordance with the requirements of this section, respond directly to the requester and, if so requested, shall notify the referring agency of the determination made on the request.

5. Freedom of Information Act Requests

Requests for declassification submitted under provisions of the Freedom of Information Act shall be processed under that Act.

6. Processing Requests for Foreign Government Information

Except as provided hereinafter, requests for mandatory review for the declassification of classified documents that contain foreign government information shall be processed and acted upon in accordance with these regulations. The USDA Agency receiving the request, if it initially received the foreign government information, shall determine whether the foreign government information in the document may be declassified and released in accordance with Department guidelines, consulting with agencies of subject matter interest as necessary. If the USDA Agency receiving the request did not initially receive the information, it shall return the information to the Department Security Officer who shall forward the information to the appropriate agency for its action. In those cases where available policy or guidelines do not apply, consultation with the foreign originator, through appropriate channels may be advisable prior to final action on the request.

7. Material in Possession of General Services Administration

Requests made to the Administrator of the General Services Administration for declassification of classified documents originated within USDA but in the possession and control of the Administrator of General Services Administration pursuant to 44 U.S.C. 2107 or 2107 note, shall be referred by the Administrator to the Department Security Officer for processing and for direct response to the requester.

8. Prohibition

No agency in possession of a classified document may, in a response to a request for the document under the Freedom of Information Act or the Mandatory Review provisions of the Order, refuse to confirm the existence or nonexistence of the document, unless the fact of its existence or nonexistence would itself be classifiable under the criteria set forth in the Order.

406 APPEALS

(a) Appeals from denial of declassification and release of information shall be directed to the Director of Personnel, Office of Personnel, Administration Building, U.S. Department of Agriculture, Washington D.C. 20250. The Director of Personnel shall act as chairperson of a Department Review Committee consisting of the Director of Personnel, the Department Security Officer and a representative of the Office of the General Counsel, the appropriate USDA Agency Head, and the head of the unit subordinate to the USDA Agency Head, who has a working knowledge of the information under consideration. The committee shall determine whether all or part of the information should be declassified and released.

(b) Appeals shall be reviewed and decided within thirty (30) days of their receipt as follows:

(1) If the documents are declassified in their entirety, the Department Security Officer shall forward the documents to the requester.

(2)(a) If the documents are not declassified and released in their entirety, the Director of Personnel shall forward a letter of denial to the requester notifying the requester of the decision and a statement of justification for the denial.

(b) If the decision of the committee is to declassify and release a portion of the documents, the Director of Personnel shall forward a letter of partial denial to the requester. The letter shall include a statement of justification for the partial denial. Those portions of the documents which have been declassified shall be forwarded to the requester.

407 CHALLENGES TO CLASSIFICATION

USDA employees having reasonable cause to believe that a document is classified unnecessarily, improperly, or for an inappropriate period of time, are encouraged to question or to challenge such classification. The employee should submit a memorandum giving the reasons to support such a challenge to the agency which originated the classification of the information, and/or may follow the procedures set forth in Sections 405 or 406. When

requested, anonimity of the challenger shall be maintained by submitting the challenge memorandum to the agency through the Department Security Officer.

408 SCHEDULE OF FEES

There will be no fees charged for mandatory review of classified material for declassification purposes.

409 DOWNGRADING

1. Automatic Downgrading

Classified information that is marked for automatic downgrading is downgraded accordingly without notification to holders.

2. Downgrading Upon Reconsideration

Classified information that is not marked for automatic downgrading may be assigned to a lower classification designation by the originator or by an official authorized to declassify the same information. Notice of the downgrading shall be provided to known holders of the information.

410 MARKING DOWNGRADED OR DECLASSIFIED DOCUMENTS

Whenever classified material is downgraded or declassified prior to the scheduled date as marked on the material, the old classification marking shall be lined through. The authority for the action and date shall be conspicuously marked to indicate the change. In the case of automatic downgrading, the original classification marking shall remain legible so that individuals other than the one effecting the change may be aware that the automatic change has been accomplished.

CHAPTER 5

Access, Dissemination, and Accountability of Classified Material

501 GENERAL POLICY

Access to classified information or dissemination of classified information orally, in writing, or by any other means, shall be limited to those persons whose official duties require knowledge or possession thereof. No one has a right to have access to classified information solely by virtue of position, grade, or security clearance.

502 GUIDELINES FOR ACCESS TO CLASSIFIED MATERIAL OR INFORMATION

1. Prior to granting access by any person to classified material or information, the person releasing the material or information shall:

(a) Establish the identity of the proposed recipient;
(b) Determine that the proposed recipient has a valid need to know the information in performance of official duty.
(c) Determine that the proposed recipient has a valid need to know the information in the performance of official duty.

2. At the time classified material or information is orally disclosed, the recipients will be informed of the category of classification of the material or information.

3. The release of classified information to a foreign government or foreign representative shall be coordinated with the Department Security Officer.

503 PROHIBITIONS FOR ACCESS TO CLASSIFIED MATERIAL FOR INFORMATION

1. Classified information shall never be revealed in a nonsecure telephone conversation, or discussed in public places, conveyances, or any place within the hearing of an unauthorized person.

2. The disclosure of classified information to relatives, friends, or other unauthorized persons may be cause for dismissal or other disciplinary action against the USDA employee involved.

3. Except as authorized in pertinent USDA issuances, no recipient of classified material or information will make a speech, write for publication, or give a course of instruction dealing with or closely related to classified material or information received by him/her by virtue of his/her official connection with USDA.

504 ACCESS BY HISTORICAL RESEARCHERS

Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information or material provided that:

1. A written determination is made that such access is clearly consistent with the interests of national security.

2. The material requested is reasonably accessible and can be located and compiled with a reasonable amount of effort.

3. The researcher agrees to safeguard the information and to authorize a review of his/her notes and manuscript for determination that no classified information is contained therein by signing a statement to this effect.

505 ACCESS BY FORMER PRESIDENTIAL APPOINTEES

Persons who previously occupied policy making positions to which they were appointed by the President, shall not remove classified material upon departure from USDA as all such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information or material which they originated, received, reviewed, signed, or which was addressed to them while in public office provided that the USDA Agency having classified jurisdiction for such information or material makes a written determination that access is consistent with the interests of national security and the person seeking access agrees:

1. To safeguard the information;

2. To authorize a review of his/her notes for determination that no classified information is contained therein;

3. That no classified information will be further disseminated or published.

506 DISSEMINATION OF CLASSIFIED INFORMATION WITHIN THE EXECUTIVE BRANCH

USDA agencies may disseminate classified information originated within USDA to another Executive Agency, but shall follow the requirements for accountability of such information or material as set forth in Section 509.

507 DISSEMINATION OF CLASSIFIED INFORMATION OUTSIDE THE EXECUTIVE BRANCH

1. Policy

(a) Classified information shall not be disseminated outside the Executive Branch without the specific

authorization of the Department Security Officer. Classified material which is to be physically released to U.S. entities outside the Executive Branch shall be marked as prescribed in Chapter 7.

(b) Information bearing the marking "Warning Notice - Sensitive Intelligence Sources and Methods Involved" shall not be disseminated in any manner outside authorized channels without the permission of the originating Department and an assessment by the Department Security Officer as to the potential risks to the national security and to the intelligence sources and methods involved.

2. Dissemination to the Congress - Provided other Departmental policies and procedures regarding legislative affairs are met, classified information may be disseminated to the Congress when necessary in the interest of the national security with the authorization of the Secretary. As used herein, the Congress includes members, committees, subcommittees, and staffs of members and committees.

3. Dissemination to Representatives of the General Accounting Office (GAO)

(a) Properly cleared and identified representatives of GAO may be granted access on a need-to-know basis to USDA classified information at USDA Agencies by each Administrator when such information is relevant to the performance of GAO statutory responsibilities and duties. The GAO will announce in advance to the visited agency the purpose of the visit, names of GAO representatives, and if access to classified information is anticipated, a certification as to the level of clearance of each representative.

(b) Requests for the following types of classified information shall be forwarded to the Administrator of each Agency, who shall consult with the Department Security Officer for determination of whether or not the information is relevant to the performance of GAO's statutory responsibilities and for authorization for release of access:

(1) Top Secret information.
(2) Other sensitive classified information falling in the general areas of tactical operations, intelligence, and communications security.
(3) Classified information originated by another department or agency of the Executive Branch, including FBI reports.

(c) When classified information is furnished to GAO representatives, they shall be informed of the classified nature of the information and of the need for safeguarding it properly. In this way, the Comptroller General has agreed to establish a security system at least equal to that prescribed by the Executive Branch.

4. Dissemination to the Government Printing Office (GPO) - Administrators of USDA Agencies may release classified material, except Top Secret and similarly unique material, to GPO plants, Washington and field, for reproduction when determined necessary for meeting printing and reproduction needs. The Public Printer has established policies and standards commensurate with those of the Executive Branch for the clearance of GPO personnel and for the safeguarding of classified information.

5. Dissemination to the Judiciary - Every effort shall be taken to prevent the disclosure of classified information in proceedings before civil courts or with legal meetings. If classified information becomes or it appears that it might become involved, the matter will be referred immediately to the Office of the General Counsel. The Office of the General Counsel in consultation with the Department Security Officer will furnish advice and guidance as appropriate to the circumstances of the situation.

508 DISSEMINATION THROUGH MEETINGS AT USDA SITES

USDA Agencies which host or convene a classified conference, symposium, seminar, exhibit, or scientific and technical gathering shall assure that security measures appropriate to the circumstances are taken. Requirements include but are not limited to the following:

1. All individuals attending the meeting shall be properly authorized and have a need for the information. All attendees may not have a need for all the information to be presented, particularly at a meeting covering a wide range of topics. In such instances, the agenda should be drawn in a manner to provide for selective attendance.

2. Attendees shall be positively identified before being admitted to the meeting room.

3. Individuals who present classified information shall be advised of any limitations on their presentations which may be necessary because of the level of clearance or need-to-know of certain members of the audience. The speaker is responsible also for seeking such guidance and for keeping his/her disclosures within the prescribed limits.

4. Notes, minutes, summaries, recordings, proceedings, reports, etc., on the classified portions of the meeting shall be safeguarded and controlled throughout the duration of the meeting. Such material, as appropriate, shall be forwarded to attendees by secure means at the conclusion of the meeting rather than being handcarried by them from the meeting site (except for local attendees).

509 ACCOUNTABILITY AND CONTROL OF CLASSIFIED MATERIAL

1. Material Subject to Accountability

(a) Each item of material that is classified Top Secret or Secret, because of its own content, is subject to accountability requirements. Such requirements do not apply to documents which are temporarily classified solely because they transmit or are attached to Top Secret or Secret documents or other material.

(b) With the following exceptions no accountability requirements are prescribed for material which is classified Confidential:

(1) Confidential cryptographic information,

(2) Confidential RESTRICTED DATA, only when the material is "documented" at the discretion of the originator to show the number of pages, series, number of copies, and individual copy number: Accountability will be maintained in conformity with the requirements set forth in this section for Secret information.

2. Designation and Responsibility of "Accountability Records Clerk" - Each USDA agency, office and/or field office which handle classified material shall designate at least one "Accountability Records Clerk" responsible for insuring the recording of all accountable material within the operating unit. All such personnel will be cleared to at least the category of security classification of the information which they process and will be adequately indoctrinated with respect to the general provisions of this Handbook and the specific requirements of this section. The designation may be omitted where the workload is such that it can be handled by the Agency Classified Material Control Officer or alternative staff member who has necessary clearance.

3. Processing Accountable Material - Each item of classified material subject to the accountability requirements of this section and which is: (1) delivered to; (2) brought into; (3) generated, reproduced, upgraded, declassified or destroyed at: (4) distributed or transferred within; or (5) transmitted or removed from the agency office shall be processed by or through the appropriate Accountability Records Clerk in accordance with such procedures as are established by the Agency Classified Material Control officer for the purpose of maintaining complete accountability records.

4. Accountability Records - Records pertaining to classified material subject to accountability will:

(a) Be afforded secure storage;

(b) Be stored apart from the material they represent: and

(c) Include the following data as appropriate:

(1) Identity of the material by title, subject or other unique description (including short title);

(2) Date originated or reproduced;

(3) Date received or dispatched;

(4) Schedule for declassification or review;

(5) Control number or identification symbol;

(6) Identity of person or office from which received and/or to which distributed within the agency, office or field office or transmitted outside the operating unit. Within a large division, office or other organizational unit, it is permissible to use an inventory log or document register to account for the internal routing of accountable information;

(7) Number of copies, series, and copy number;

(8) Date, new classification (or lack thereof), an authority for upgrading, downgrading, or declassification action; and

(9) Date of destruction and authority for destruction.

5. Classified Material Receipts - A Classified Material Control Receipt, (AD-471) will be used to transmit accountable material outside the Department. Within the Department a receipt or charge-out system of accountability may be used. A charge-out card may be used in conjunction with a receipt when the material is loaned or routed within the agency for a short period of time. Under such a system, a file charge-out card may be substituted for the material and indicate the name and location of the person receiving the material and the date. For inventory purposes, the last person signing the USDA receipt should be considered the custodian of the material.

6. Inventory of Accountable Material - A physical inventory of all Top Secret material shall be made at least annually. As an exception, repositories storing large volumes of classified material shall develop inventory lists or other finding aids.

7. Accountable Material Not Under Accountability - Each person who receives or has in his/her possession classified material which has not, but should have been, entered into the accountability system of the agency will promptly notify the Agency Classified Material Control Officer and cause a record of the material to be made in the accountability records.

8. Restrictions on Possession or Use of Classified Material

(a) Classified material at each USDA agency office or field office shall be either under the immediate, continuing control and supervision of an authorized person or stored in an approved manner as provided in this Handbook. The same requirements apply, without exception, to classified material that is removed from a USDA agency, office or field office for use at official conferences, transmittal to authorized recipients, or other necessary official purposes.

(b) Only in cases of clear necessity, approved in advance by the Agency Classified Material Control Officer, will classified material be removed to or retained in the temporary or permanent residence of a USDA employee. This provision includes classified material personally transported by an employee while on official travel. Official documentation of the approval of any such temporary or continuing arrangement will be provided on a timely basis to the Agency Classified Material Control Officer. As a minimum, the documentation will specify:

(1) Official necessity with exceptional arrangements:

(2) Precise means by which the classified material will be continuously safeguarded while outside the confines of the agency, as required in Subparagraph a:

(3) The precise means by which strict accountability will be maintained concerning each item of classified material removed, returned, or otherwise disposed of under the arrangement.

(c) Classified material will not be exposed or utilized under circumstances which present an opportunity for physical or visual access to the contents by an unauthorized person. Exposure of use of classified material in public areas, including public areas on common carriers, vehicles, is specifically prohibited.

(d) Cryptographic material, RESTRICTED DATA, or information from a foreign government or international pact organization will not be removed to a temporary or permanent residence unless specifically required in connection with official travel. When such material is removed, all the provisions in Subparagraphs b and c will apply.

(e) Whenever classified material is in actual use by an authorized person, the material will be:

(1) Kept under the immediate, continuing control and supervision of an authorized person;

(2) Covered, turned face down, placed in security storage equipment or in a controlled area, or otherwise adequately protected whenever an unauthorized person is present;

(3) Placed in security storage equipment or in a controlled area as soon as practicable after use.

CHAPTER 6

Storage of Classified Material

601 GENERAL POLICY

Classified material may be used, held, or stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it. The exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances. They must allow the accomplishment of essential functions while affording classified material reasonable and appropriate degrees of security, with a minimum of risk. The requirements specified in this Handbook represent the minimum acceptable standards.

602 UTILIZATION AND PURCHASE OF SECURITY STORAGE EQUIPMENT

(1) Security Storage equipment should not normally be used for the storage of unclassified documents, personal articles of significant value, or other materials. Each USDA supervisor
should establish and maintain a program which provides for the continuing review of classified material on hand for the purpose of reducing and maintaining at an absolute minimum the quantity of such material on hand at any given time.

(2) Prior to purchasing new security storage equipment already available within USDA through the consolidation or disposal of the existing records and other stored materials.

(3) Whenever it becomes necessary to purchase new filing equipment for the storage of classified material it will be, to the maximum extent practicable, of the type designated as "security filing cabinets" on the Federal Supply Schedule of the General Services Administration.

603 STORAGE OF VARIOUS CATEGORIES OF CLASSIFIED MATERIAL

1. Top Secret Material - Top Secret material shall be stored in a safe or safe-type steel file container having a built in three-position dial-type combination lock, vault, or vault-type room, or other storage facility which meets the standards for Top Secret established under the provisions of Section 602, and which minimizes the possibility of unauthorized access to, or the physical theft of, such material. All corridor doors of a room where Top Secret material is stored shall be locked when the room is unoccupied.

2. Secret and Confidential Material - Secret and Confidential material may be stored in a manner authorized for Top Secret material or in a steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA approved changeable combination padlock. Where Secret material is stored, all corridor doors should be locked when the room is unoccupied.

3. Storage of Classified Cryptographic Material - Classified cryptographic information will be stored in conformity with requirements established by the Department Security Officer on a case-by-case basis.

4. Storage of Restricted Data and Formerly Restricted Data - Restricted data and formerly restricted data will be stored in conformity with requirements of Paragraph 1 or 2 as appropriate for the specific level of security classification on the material itself.

5. Storage of Hazardous or Bulky Classified Material - When, due to its nature or size, it is hazardous or otherwise impractical to store classified material in accordance with the usual requirements, the material will be stored within a controlled area which has been specifically approved for this purpose by the Department Security Officer. To insure continuity of safeguarding, such material will be removed from the controlled area only under conditions specifically approved by the Department Security Officer.

6. Storage of Classified Waste and Reproduction Materials - Pending actual destruction, all waste and reproduction materials which contain classified information will be stored in conformity with the requirements of Paragraphs 1 and 2, as appropriate, for the specific level of security classification of the information involved.

7. Storage of Material Marked Limited Official Use (LOU) - Officially limited information is important, delicate, sensitive or proprietary information which is provided to this Department usually by the Department of State offices, both domestic and from embassies or posts in foreign countries. Information marked LOU is not classified information under the criteria of the Order, but its use and distribution must be restricted to officials who have a need to know. Information so marked shall be handled, safeguarded. amd stored in a manner equivalent to information classified CONFIDENTIAL.

CHAPTER 7

Protection of Security Storage Equipment and Controlled Area

701 INSPECTION

Agency Classified Material Control Officers will thoroughly inspect security storage equipment and controlled areas at times and under conditions prescribed by the Department Security Officer to insure that the equipment in areas are adequately secured or otherwise protected during both work and non-work hours. If any storage equipment, controlled area, or classified material is found not to be protected in accordance with the requirements of this Handbook, the Department Security Officer will be notified and corrective action taken in compliance with such procedures as he/she may establish.

702 RESTRICTION AND USE OF SECURITY STORAGE EQUIPMENT AND CONTROLLED AREAS

To minimize the possibility of compromise of classified information as an incidence to attempt to break and enter security storage equipment or a controlled area, such items as money, weapons, narcotics and precious metals will not be stored during non-working hours in any security storage equipment or controlled area in which classified material or information is stored. This restriction does not apply to intrinsically valuable material which by their own nature are classified or are properly a part of a component of classified hardware. The restriction may be waived in an emergency, provided action is initiated promptly to provide other storage arrangements for the restricted item(s).

703 DESIGNATION AND RESPONSIBILITIES OF CUSTODIAN OF SECURITY STORAGE EQUIPMENT OR CONTROLLED AREAS

A primary custodian will be designated for each unit of security storage equipment and each controlled area by the responsible supervisor; the same individual may be custodian of a group of such units. The identity of each custodian shall be made known to the Agency Classified Material Control Officer by such means as he/she may establish. Non-USDA employees such as contractor personnel, assigned to an office in direct support of a USDA activity may be designated custodian provided all pertinent requirements of this Handbook are met. Each custodian will be responsible for insuring that:

(1) The security storage equipment is securely locked or that the controlled area is maintained under all security measures established by the Department Security Officer whenever the equipment or area is not under the immediate continuing supervision and control of an authorized person.

(2) Locking devices are in good order and that combinations are changed, as a minimum, in accordance with the requirements set forth in Section 707.

704 PROTECTION OF COMBINATION PADLOCK

Each combination padlock used for security storage equipment or a controlled area should be placed in a drawer or locked to the hasp whenever the equipment area is open.

705 KNOWLEDGE OF LOCKING DEVICE COMBINATION

1. Knowledge of the combination of a locking device used to secure classified material will be limited to the minimum number of persons actually required to effectively maintain normal business operations.

2. The identity of each individual having knowledge of the combination will be made known to the Agency Classified Material Control Officer by such means as he/she establishes.

3. The Agency Classified Material Control Officer should deposit the combination to his/her safe in the Office of the Department Security Officer.

706 RECORD OF LOCKING DEVICE COMBINATION

A record of lock and padlock combination used in connection with the storage of classified material will be made only when it is not practical to memorize the combinations due to the number of locking devices involved. Such a record will be:

1. Classified no lower than the highest category of classified material authorized for storage in any equipment concerned and will be higher if the overall accumulation of Confidential or Secret material warrants the protection afforded information of a higher category of security classification.

2. Stored in conformity with the requirements of Section 603-1 and 2, according to the category of security classification involved.

707 CHANGE OF LOCKING DEVICE COMBINATION

The combination of a lock or padlock used for security purposes shall be changed:

1. When the locking device is first placed in use;

2. Whenever a person having knowledge of the combination is transferred, terminates employment or for some other reason is no longer authorized access to the classified information stored in the equipment or area;

3. Whenever the combination is believed to have been subject to compromise;

4. Whenever the security storage equipment or controlled area has been found unsecured and unattended by an authorized person; and

5. At least once every 12 months.

CHAPTER 8

Reproduction of Classified Material

801 GENERAL PROVISIONS

1. Top Secret, Secret, or Confidential material originating in another government agency or department shall not be reproduced without the written consent of the individual of that agency or department having authority to approve such reproduction.

2. Reproduced copies of classified material are subject to the same accountability and controls as the original documents.

3. Records shall be maintained by all USDA agencies that produce paper copies of classified material to show the number and distribution of reproduced copies of all classified material, of all documents covered by special access programs distributed outside the originating agency, and all documents which are marked with special dissemination and reproduction limitations.

4. Any reproduction must be for use only within USDA.

5. Section 901-1 shall not restrict the reproduction of documents for the purpose of facilitating review for declassification. However, such reproduced documents that remain classified after review must be destroyed after they are used.

CHAPTER 9

Transmission of Classified Information and Material

901 PREPARATION FOR TRANSMISSION

1. Outside a USDA Agency or Field Office - Classified material being prepared for transmission outside a USDA agency or field office will be securely enclosed in sealed, opaque inner and outer envelopes or other types of covers of sufficient strength to withstand rough handling. The address and return address will be placed on both covers,. The highest category of security classification of its contents will be plainly marked only on the inner cover and will include, when appropriate, the additional marking of "RESTRICTED DATA." The outer cover will bear no indication of the classification or the RESTRICTED DATA nature of its contents. Whenever, due to its nature, weight, or size, classified material cannot be prepared for transmission as indicated in this paragraph, it will be prepared in accordance with specific instructions obtained from the Agency Classified Material Control Officer, or Department Security Officer. Whenever any doubt exists as to the authorized safeguarding and storage capability of any intended recipient of classified material, the Department Security Officer will be consulted in advance.

2. Within a USDA Agency or Field Office - Classified material being prepared for transmission entirely within an individual USDA office or field office, as a minimum, will be afforded the protection of an appropriate classified cover sheet. Additional measures may be established by the Agency Classified Material Control Officer to prevent unauthorized access.

3. Classified Material Control Receipt (AD-471)

(a) An AD-471 classified material control receipt will be prepared for all Top Secret and Secret material, except that a charge-out system may be used in lieu of a receipt within an individual agency. Confidential material will require a receipt only if preceding requirements for a particular item have been established previously or a sender otherwise deems it necessary. The receipt form will contain no classified information.

(b) An AD-471 classified material control receipt normally shall be attached to or enclosed in the inner cover. When necessary, the receipt may be forwarded in any other manner approved by the Agency Classified Material Control Officer.

(c) A copy of the AD-471 classified material control receipt and a record of the mail registry or other identification symbol shall be retained pending return of the signed receipt. If a receipt is not returned within a reasonable time, follow up inquiry shall be made.

902 TRANSMISSION OF TOP SECRET INFORMATION

1. The transmission of Top Secret information shall be effected preferably by oral discussion in person between the officials concerned, in an appropriately secured area. Otherwise the transmission of Top Secret information shall be by specifically designated personnel, by State Department diplomatic pouch, by a messenger-courier system especially created for the purpose, over authorized communications circuits in encrypted form or by other means authorized by the Department Security Officer.

903 TRANSMISSION OF SECRET AND CONFIDENTIAL INFORMATION

1. Secret or Confidential information may be transmitted within the United States by one of the means authorized for Top Secret information, by the United States Postal Service registered mail, and by protective services provided by United States commercial carriers under conditions prescribed by the Department Security Officer.

2. Canadian Government Installations - Secret and Confidential information may be transmitted to and between USDA and Canadian Government installations by United States and Canadian registered mail with registered mail receipt.

3. Transmission to Other Foreign Countries - Secret and Confidential information may be transmitted to United States Embassies or installations by:

(a) Handcarried by specifically designated USDA employees who possess an appropriate security clearance and have been briefed on specific responsibilities;

(b) State Department diplomatic pouch;

(c) A messenger-courier system especially created for the purpose (such as the Armed Forces Courier Service);

(d) Electric means in encrypted form;

(e) Commanders or masters of vessels of United States registry;

(f) Registered United States mail through Army, Navy, Air Force, or United States civil postal facilities; provided that the information does not pass out of the U.S. Government control and does not pass through a foreign postal system. Registered mail in the custody of transporting agency of the United States Post Officer is considered, for the purpose, to be within the U.S. Government control unless the transporting agent is foreign controlled or operated.

904 METHODS OF TRANSMISSION WITHIN USDA NATIONAL HEADQUARTERS, AN AGENCY, OFFICE OR FIELD OFFICE

1. Hand-delivered by an employee possessing a clearance at least as high as the category of classification of the material involved.

2. Through the internal mail distribution system, in accordance with the procedures approved by the Agency Classified Material Control Officer or Department Security Officer.

905 TRANSMISSION OF CRYPTOGRAPHIC INFORMATION

The transmission of cryptographic information, in each instance, shall be in accordance with specific guidance obtained from the Department Security Officer.

Chapter 10

Disposition or Destruction of Classified Information

1001 GENERAL

1. The provisions of this Chapter apply generally to the routine disposition or destruction of classified material. When a particular document contains specific instructions to the contrary, however, those specific instructions shall be followed.

2. When doubt exists as to the propriety of destroying classified material received from another Federal department or agency, the material shall be returned to, or permission to destroy the material obtained from, that department or agency.

3. To prevent an unnecessary accumulation of classified material, all superseded classified documents (except record copies) and all copies of classified documents surplus to the actual needs of the office, agency, or installation will be disposed of or destroyed as rapidly as practicable.

4. All classified material, including waste and reproduction materials containing classified information, shall be safeguarded as prescribed in this Handbook for the specific category of security classification involved until the material is actually disposed of or destroyed.

1002 TOP SECRET MATERIAL

Top Secret material (including Top Secret RESTRICTED DATA) shall be disposed of either by returning to the originating office or delivery to the Department Security Officer for destruction.

1003 CLASSIFIED CRYPTOGRAPHIC MATERIAL

Material embodying classified cryptographic information shall be disposed of or destroyed by reporting to the Foreign Agricultural Service, Management Services Division.

1004 DESTRUCTION OF CLASSIFIED MATERIAL

1. General

(a) Destruction may be limited to those components or portions of material or equipment which actually incorporate classified information.

(b) Classified information embodied in paper products shall be destroyed by burning (with pulverization of the residue), by pulping, or by shredding or pulverization of the material in an unrecognizable form and beyond reconstruction in whole or in part.

(c) Classified information embodied in material other than paper products shall be destroyed by any method specifically approved by the Department Security Officer as having the capability of completely and permanently rendering the information indistinguishable and incapable of being reconstructed in whole or in part.

2. Witnessing and Certifying Destruction

(a) The requirements of Subparagraph 1b above pertain only to (1) Secret information (including RESTRICTED DATA) generated by any Federal department or agency; and (2) Confidential RESTRICTED DATA, only when the material is "documented" (to show number of pages, series, number of copies, and individual copy number).

(b) Classified material stipulated in Subparagraph 2a which is eligible for destruction shall be destroyed by at least two persons; all persons participating must possess that appropriate degree of security clearance. At least one of these persons should be a permanent USDA employee who:

(1) Has been designated by the Agency Classified Material Control Officer to supervise and witness the destruction;

(2) Has been adequately briefed in the pertinent requirments of this Handbook; and

(3) Will certify destruction of the material.

(c) Records of destruction shall be maintained for a minimum of two years after when they may be destroyed.

Chapter 11

Security Violations and Compromise of Classified Material and Information

1101 GENERAL

Classified material and information is vulnerable to compromise whenever its custodian allows himself/herself to become negligent; for example:

1. Failing to properly secure classified material when not under his/her immediate, continuing control and supervision;

2. Not properly preparing the material for transmission, or improperly transmitting the material within or outside the agency;

3. Discussing or attempting to "talk around" classified information during telephone conversations or in places where unauthorized persons are present;

4. Misplacing or otherwise losing control of classified material (including classified waste); or

5. Releasing classified material and information without properly determining the recipient's identity, clearance status, and need-to-know.

1102 EMERGENCY ACTION AND REPORTING REQUIREMENTS

1. Whenever any individual observes that classified material and information is not being afforded the prescribed protection that individual will:

(a) Immediately take all interim action possible to restore the prescribed security controls over the information or material.

(b) Report the circumstances promptly to his/her immediate supervisor or, if not immediately available, directly to the Agency Classified Material Control Officer. Non-USDA personnel having no immediate superior within a USDA agency or office or a component activity will report the circumstances as prescribed by the Agency Classified Material Control Officer.

1103 ACTION TO BE TAKEN BY THE AGENCY CLASSIFIED MATERIAL CONTROL OFFICER

1. Preliminary Action and Inquiry - Upon becoming aware that there has been a loss of prescribed security control over classified material and information, the Agency Classified Material Control Officer will take appropriate action to:

(a) Insure that all required security controls over the information or material actually have been fully restored;

(b) Insure that all classified material involved is accounted for by the custodian(s) as expeditiously as possible; whenever Top Secret material is involved, however, an inventory will be conducted immediately;

(c) Provide for the immediate change of each locking device combination which may have been subject to compromise; and

(d) Determine whether a compromise of classified information or material may have occurred.

2. Action Required in Event Classified Material and Information was not Compromised - If the preliminary inquiry indicates that information or material was not subject to compromise, but that a security violation did occur, the Agency Classified Material Control Officer will:

(a) Determine the circumstances surrounding the security violation and the identity of the individual(s) responsible:

(b) Obtain a written account of the violation from the responsible individual(s);

(c) Provide copies of the report containing essential details of the incident to the Department Security Officer;

(d) Take corrective action to eliminate the practice or condition that caused or permitted the security violation.

3. Action Required in Event of Possible Loss or Compromise of Classified Material and Information

(a) If the preliminary inquiry indicates that classified material is missing or lost, or that classified information has been otherwise subjected to compromise, the Agency Classified Material Control Officer shall:

(1) Report the circumstances to the Department Security Officer;

(2) Complete identification of each item of classified information involved and so inform the Department Security Officer;

(3) Conduct a thorough search for the missing classified material;

(4) Forward a written report to the Department Security Officer identifying the person(s) and procedure(s) deficiency which caused the compromise. The report will include an explanation by the person(s) responsible for the compromise.

(b) The Department Security Officer will effect all liaison with other Federal departments in the event of possible loss or compromise of classified material or information.

(c) Agency heads shall assure that prompt and appropriate personnel administrative action is taken whenever any USDA employee is determined to have been knowingly responsible for any release or disclosure of classified information or material except in a manner authorized by statute, protective order or established regulation.

1104 ACTION REQUIRED IN EVENT OF POSSIBLE LOSS OR COMPROMISE OF CLASSIFIED NATO INFORMATION

The Department Security Officer, subsequent to notification by a USDA agency responsible for safeguarding classified NATO information, shall submit an initial report of the incident to the United States Security Authority for NATO Affairs (USSA) and shall initiate investigation in accordance with the provisions of USSA instructions.

CHAPTER 12

Security Education Program

1201 RESPONSIBILITY AND PURPOSE

All USDA employees who hold security clearances and occupy critical or noncritical sensitive positions do not require access to classified information or material. Those USDA employees who are entrusted with classified information or material must be made aware of their responsibilities. Each Agency Classified Material Control Officer shall establish a security education program to indoctrinate employees involved with classified information in their security responsibilities. Such a program shall stress, among other things, the objective of declassifying more information, protecting better that which requires protection, and the purposes of Executive Order 12065 as they apply to USDA employees.

1202 SCOPE AND PRINCIPLES

1. The security education program shall include all USDA personnel entrusted with classified information regardless of their position or grade. Each Agency Classified Material Control Officer shall design his/her program to fit the particular requirements of the different groups of personnel who have access to classified information. Emphasis must be placed on the achievement of the real goals of the program. Each program shall include all or most of the following:

(a) Advise employees of the need for protecting classified information, the adverse effects to the national security that could result from unauthorized disclosure, and their personal responsibility for safeguarding classified information in their possession.

(b) Indoctrinate employees fully in the principles, criteria, and procedures for derivative classification, downgrading and declassification, including appropriate marking, of the information as prescribed in this Handbook. Employees should be alerted to the strict prohibitions on improper use and abuses o the classification and declassification systems.

(c) Familiarize employees with procedures for challenging classification decisions believed to be improper and/or an overly long period for continued classification has been assigned.

(d) Familiarize employees with the specific security requirements of their particular assignment.

(e) Inform employees of their responsibility to report any suspicious act that may be considered an attempt by foreign intelligence agents to obtain classified information.

(f) Advise employees of the hazards involved and the strict prohibitions against discussing classified information over the telephone, or in such a manner as to be intercepted or overheard by unauthorized persons.

(g) Inform employees that disciplinary actions may result from violation, neglect, or disregard of Executive Order 12065 and any implementing directives of this Handbook.

(h) Instruct employees that prior to disseminating classified information, they must determine that the prospective recipient (1) has been cleared for access, (2) needs the information in order to perform his/her official duties, and (3) can properly protect (or store) the information.

2. When indoctrinating employees assigned to duties requiring access to classified information, the Agency Classified Material Control Officer should utilize this Handbook and the Department Security Officer's memorandum dated March 2, 1981, subject: "Security Responsibilities For All Employees Cleared to Handle Defense Classified Information Vital to National Security."

1203 FOREIGN TRAVEL BRIEFING

Employees whether they have or have not had access to classified information shall be given a "foreign travel briefing" as a defensive measure prior to travel to Russia and the Peoples Republic of China (PRC). Employees who frequently travel to the two countries need not be briefed for each such occasion. A thorough briefing at least once each six months shall suffice.

1204 DEBRIEFINGS

Upon termination of employment at USDA or reassignment to USDA duties designated nonsensitive, employees shall be debriefed by the Agency Classified Material Officer or an agency employee designated by him/her. The affected employee shall return all classified material and shall execute a Security Debriefing Secrecy Agreement (AD-491) which shall be forwarded to the Department Security Officer.

Chapter 13

Program Management

1301 GENERAL

The Administrator of General Services assisted by the Information Security Oversight Officer (ISOO), is charged by Exeacutive Order 12065 to monitor compliance with the provisions of the Executive Order and with such supplementing directives as the National Security Council may promulgate. The ISOO has a full-time director appointed by the Administrator of General Services subject to approval by the President.

1302 FUNCTIONS OF THE DIRECTOR OF THE ISOO

1. The Director of the ISOO is charged with the following principal functions which pertain to USDA:

(a) Oversee USDA actions to ensure compliance with Executive Order 12065 and implementing directives.

(b) Consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program including appeals from decisions on declassification requests.

(c) Report annually to the President through the Administrator of General Services and the National Security Council on the implmentation of Executive Order 12065.

(d) Review all USDA implementing regulations and guidelines for systematic declassification review.

(e) Conduct on-site reviews of the information security program of each USDA agency that handles classified material.

2. The Director of the ISOO is authorized to request information or material concerning USDA as needed by the ISOO in carrying out its functions.

1303 AGENCY RESPONSIBILITY

1. The head of each agency shall direct the Agency Classified Material Control Officer to report any of the following violations of Executive Order 12065 to the Department Security Officer:

(a) Knowing and willful classification or continuing the classification of information in violation of the Executive Order or the provisions of the Handbook.

(b) Knowingly, willfuly and without authorization disclose properly classified information by communications or physical transfer to an unauthorized person or compromise properly classified information through negligence.

(c) Knowingly and willfully violate any other provision of Executive Order 12065 or this Handbook.

1304 ADMINISTRATIVE SANCTIONS

ALL USDA employees are subject to administrative sanctions such as a warning, reprimand, suspension without pay, or removal when it is determined that violations have occurred and corrective action is necessary.

Example Page 1

THIS SAMPLE MEMORANDUM DOES NOT CONTAIN CLASSIFIED INFORMATION

CONFIDENTIAL [1]/

United States Department of Agriculture [2]/

Office of the Secretary

Washington, D.C. 20250

November 30, 1978 [3]/

SUBJECT: Minimum Required Markings for Classified Documents (u)[4]/

TO: All Executive Branch Agencies

[9]/(c) Each portion of a classified document shall be marked to indicate the highest classification of information it contains. For example, this paragraph is marked as if it contained CONFIDENTIAL information.

(u) The bracketed numbers on this page indicate those markings required for all classified documents. The footnotes refer to the appropriate paragraph of this Handbook.

(u) Other markings shall be applied to classified material depending on the content:

A determination that information should be downgraded automatically (Section 305-2(a)(3))

A document that does not contain classified material but is used to transmit classified material (Section 305-3)

A document that contains foreign government information (Section 305-4)

A document that contains restricted Data or Formerly Restricted Data (Section 305-2(c)(1)(2))

A document that contains information on sensitive intelligence sources and methods (Section 305-2(c)(3))

CONFIDENTIAL

A determination that information requires limitations on reproduction and/or dissemination (Section 305-2(b))

Classified by [5]/

Review for declassification on [6]/

Extended by [7]/

Reason for Extension [8]/

Footnotes

1/ Page Markings-Section 305-2(a)(4)
2/ Office of Origin-Section 305-2(a)(2)
3/ Date of Derivative Classification-Section 305-2(a)(2)
4/ Subjects and Titles-Section 305-2(e)(1)
5/ Identity of Classifier or Classification Guide-Section 305-2(a)(1)
6/ Date/Event for Declassification/Review (check appropriate block)-Section 305-2(a)(3)
7/ & 8/ Extension: Authority and Reason-Section 305-2(a)(5)
9/ Mandatory Portion Marking-Section 305-2(e)

CONFIDENTIAL

*U.S. GOVERNMENT PRINTING OFFICE: 1981-0-730-290/2246